Lecture 15

In this lecture we finish our introductory look at logic, and we begin our study of algorithms.

Equivalence

$$\Longleftrightarrow$$

We say <u>P is equivalent to Q</u> and write

$$P \Longleftrightarrow Q$$

if whenever P is true, Q is true, and also whenever Q is true, P is true.

Note: some texts use

$$\longleftrightarrow$$

instead of $\Longleftrightarrow$.

In words:

P is equivalent to Q

P $\underbrace{\text{if and only if}}_{\text{iff}}$ Q

P is necessary & sufficient for Q

Eg. Which of the following are true?

- Some integers are real numbers. **True**
- "Most" integers are real numbers. **True ?**
- All integers are real numbers. **True**
- Some real numbers are irrational. **True**
- All real numbers are irrational. **False**

__Note__ $P \Longleftrightarrow Q$ means $\left\{\begin{array}{l} P \Longrightarrow Q \\ \text{and} \\ P \Longleftarrow Q . \end{array}\right.$

"is implied by"

__Eg.__ $3 > 2 \Longleftrightarrow 2 < 3$ [True]

$2 < 3 \Longleftrightarrow 2 < 1$ [False]

Algorithms

As previously mentioned, an <u>algorithm</u> is a systematic procedure for solving some kind of problem.

Algorithms are basic to computer programs. Essentially, a program implements one or more algorithms.

This is why algorithmic complexity is important. (But it's a difficult topic.)

We will study a few algorithms.

The Division Algorithm

Let a, b be integers. Suppose $b > 0$. Then there exist integers q and r such that

$$a = bq + r$$

where $0 \leq r < b$.

We call q the <u>quotient</u> and r the <u>remainder</u> in the division of a by b.

The process of expressing a in this way is the application of the <u>division algorithm</u>.

Essentially this says that we can divide one integer by another if the latter is positive, and that we get a quotient and a remainder.

If $a > 0$, then

$$q = \left\lfloor a/b \right\rfloor. \qquad \text{(floor of } a/b\text{)}.$$

Eg. $a = 31$, $b = 7$

$$q = \left\lfloor 31/7 \right\rfloor = \left\lfloor 4\tfrac{3}{7} \right\rfloor = \left\lfloor 4.\dot{4}2857\dot{1} \right\rfloor$$
$$= 4$$

So $a = bq + r$

gives $31 = 7 \cdot 4 + \boxed{3}$.

Given a, b:

> Valid input requires a, b to be integers and $b > 0$.

$$q = \lfloor a/b \rfloor$$

$$r = a - bq$$

<u>Euclidean Algorithm</u>

Let a, b and c be integers.

Suppose that $a \cdot b = c$.

Then c is the <u>product</u> of a and b.

Also, a and b are <u>divisors</u> or <u>factors</u> of c.

We also say that c is a <u>multiple</u> of a (and also of b).

Let m, n be positive integers. A positive integer c is a <u>common factor</u> or <u>common divisor</u> of m and n if it divides (is a divisor, or factor, of) both of them.

A positive integer d is a <u>common multiple</u> of m and n if it is a multiple of both of them.

The gcd (<u>greatest common divisor</u>) of m and n is the greatest no. which is a common divisor of both of them.

It's also called the <u>highest common factor</u> or hcf.

<u>E.g.</u> 18, 24

$$\gcd(18, 24) = \boxed{\quad}$$

Answer is 6.

There is a systematic procedure for getting the gcd. It's the Euclidean algorithm.